Deloitte.

사이버의 미래 2023 서베이

비즈니스의 중심, 사이버

Deloitte Global

2023년 02월
Deloitte Insights

카카오채널 바로가기

답은 사이버다

오늘날 '사이버'(cyber)에 대한 시선이 달라지고 있다. 리더들은 사이버를 예리한 시선으로 바라보며 사이버를 통해 얻을 수 있는 비즈니스 가치를 내다보고 있다. 사이버는 이제 성장 전략의 중심축이 되었다.

사이버는 더 이상 단순히 의무나 기술 중심의 사이버 보안 업무에 그치지 않는다. 사이버는 이를 넘어 기업들이 성과를 내는 데 도움을 주는 중요한 요소가 되었다. 그리고 딜로이트의 '사이버의 미래 2023 서베이' 결과는 이를 방증한다. 딜로이트가 실시한 사이버 서베이 중 가장 규모가 큰 올해 글로벌 서베이는 다양한 산업의 리더들을 대상으로 설문을 진행해 사이버의 현황과 나아가고 있는 방향을 살펴보고자 했다. 조사 결과 사이버는 '인에이블러'(enabler)로서 성장하고 있는 것으로 나타났다. 사이버는 기업의 규모와 상관없이 주요 아젠다로 자리 잡아가고 있으며 중요한 사업 이니셔티브와 투자가 사이버에 초점이 맞춰져 있다.

사이버의 미래는 흥미진진하다. 본 보고서는 서베이 결과에서 도출한 데이터 외에 서베이 응답자들의 논평과 인사이트도 포함한다. 또한 기업의 미래를 좌우할 사이버, 클라우드, 기타 다른 기술에 대한 딜로이트의 통찰력을 담았다.

Emily Mossburg
딜로이트 글로벌 사이버 리더

목차

사이버, 그 너머

사이버의 미래에 대한 관심이 뜨겁다. 전 세계 기업들이 기술과 사이버 위협에만 집중하던 양상에서 벗어나고 있다. 기업들은 전사적으로 사이버 사고와 행동 양식을 심층적으로 받아들임으로써 이룰 수 있는 긍정적인 효과에 초점을 맞추고 있다.

세계는 점점 더 연결되고 있다. 이는 새로운 성장 기회를 가져오지만 새로운 리스크 또한 불러온다. 새로운 디지털 기술이 등장하고 데이터가 기하급수적으로 증가하며 비즈니스 니즈가 변화함에 따라 공격 노출면(attack surface)이 넓어지고 있으며 새로운 과제가 생겨나고 있어, 사이버가 비즈니스 전략 이슈로 떠오르고 있다. 사이버 위협을 무력화하고 기업 가치를 보호하며 소비자의 신뢰를 지키기 위해서는 사이버, 리스크 관리, 사업 부서 간의 협업이 중요하다.

최근 몇 년간 다수의 기업 리더들이 비즈니스 프로세스를 지속적으로 디지털화하는 데 초점을 맞추고 있으며 이와 더불어 기술 환경과 사이버 위협의 급속한 진화에 집중하고 있다. 실제로 하이브리드 IT와 디지털 전환을 관리하는 것이 기업들이 직면하고 있는 가장 큰 과제로 부상했다. 기업들에게 복잡함이 일상이 된 것이다[1].

딜로이트 글로벌 사이버의 미래 2023 서베이에 따르면 오늘날 상황이 완전히 바뀌고 있다. 본 서베이는 전 세계 다양한 산업에 종사하는 수백 명의 리더들에게 사이버 위협과 기업 활동, 미래에 대해 의견을 물었다. 이 서베이에는 C레벨 임원진뿐만 아니라 IT와 보안, 리스크를 담당하는 고위 경영진도 참여했다.

사이버는 기업의 한 전문 부서로 거듭나고 있다. 기존에 사이버는 IT 부서의 한 영역이었으나 이제는 이를 넘어 비즈니스 성과를 달성하기 위한 프레임워크의 필수적인 부분이 되고 있다.

인식의 전환

"저희는 사이버 보안을 사업적 리스크로 보며 이전보다 훨씬 더 사이버 보안에 신경을 쓰기 시작했습니다. 전사적으로 사이버 보안을 부차적인 문제로 보는 인식에서 벗어나고 있으며 당사 트랜스포메이션의 핵심 요소로 인식하기 시작했습니다. 데브섹옵스(DevSecOps)든 제품 개발에 있어서든 사이버를 수용하기 위해 힘을 쏟고 있습니다. 저희는 안전하게 구축할 수 있도록 내부 파트너들과 함께 작업하기 시작했습니다. 문화적 변화와 같죠."

쉘(Shell)사 CIO/CISO 앨런 콕리얼

사이버는 기업의
한 전문 부서로 거듭나고 있다.
기존에 사이버는 IT 부서의
한 영역이었으나
이제는 이를 넘어 비즈니스 성과를
달성하기 위한 프레임워크의
필수적인 부분이 되고 있다.

기업들은 사업 성공에 있어 사이버의 중요성을 인식하고 있다.

2023년과 그 이후를 내다봤을 때 사이버는 기술 그 이상으로 성장하고 있다. 많은 기업의 경우 사이버는 이제 사업 운영과 성과, 기회에 밀접하게 연결되어 있다. 사이버 관련 의사 결정자 사이에서 사이버는 사업 구조의 일부가 되었으며 사업 목표를 이루기 위한 요소이다.

IT 영역의 문제에 그쳤던 사이버 위협이 이제는 비즈니스상의 문제가 된 것처럼, 사이버 전략 또한 IT에 국한하지 않는 비즈니스 전략이 되었다. 궁극적으로 비즈니스 전략 목표와 성장에 일조하는 것이다. 사이버는 사업상 우선순위로서 이사회 차원에서 중요하게 다뤄지고 있다. 올해 서베이에서는 응답자의 70%가 사이버가 월별 또는 분기별로 이사회 안건에 올라간다고 응답했다. 중요한 전략적 비즈니스 의사 결정이 이루어지는 테이블에서 사이버가 중요한 위치를 차지하는 것이다.

기업들은 사업 성공에 있어 사이버의 중요성을 인식하고 있다.

대다수의 설문 응답자는 사이버와 경영 성과 사이에 강력한 연관성이 있다고 답했다. 이중 86%는 사이버 이니셔티브가 하나 이상의 주요 비즈니스 영역에 긍정적으로 기여했다고 응답했다. 따라서 대부분의 기업이 사이버에 관심을 가지고 있으며, 58%가 내년에 사이버 투자를 늘릴 계획이다.

사이버에 익숙해진 이사회

"이사회들이 사이버 보안에 관심을 쏟고 있습니다. 놀라운 수준으로 많은 자원을 사이버 보안에 할당할 거예요. 이사회들은 이제 유능한 보안 리더십이 어디에 있는지, 그리고 누가 문제 상황을 해결하고 있는지 파악할 정도의 충분한 교육을 받았습니다. 이들이 그 차별성을 인식하게 된다면 고위 임원과 이사회의 수용성이 커질 겁니다."

소비재 기업 CISO

70%가
월별 또는 분기별로
사이버가 이사회 안건에 올라간다고 응답

사이버는 '비즈니스를 가능하게 하는 요소', 즉 비즈니스 인에이블러(business enabler)로서의 잠재력이 있으나, 사이버를 효과적으로 활용할 수 있는 능력은 기업마다 천차만별일 수 있다. 일부 기업들은 다른 기업들이 벤치마킹할 수 있는 선두 주자로 부상했다.

올해 서베이에서 딜로이트는 사이버 계획의 수준, 이사회 차원의 논의, 사이버에 대한 전략적 조치의 수준을 기준으로 성숙한 기업을 파악했다. 이러한 기업들은 사이버 보안에 중요한 조치를 모두 이행하고 있다. 중요한 조치에는 운영 및 전략 계획, 기업의 정보 보안을 지속적으로 개선하는 조치 계획, 파트너사와 공급업체의 보안 상태를 모니터링하고 추적하기 위한 사이버 리스크 프로그램 등이 있다.

성숙도가 높은 기업들이 사이버에 쏟는 노력은 특히나 비즈니스 가치로 이어지고 있다. 이들의 사이버 이니셔티브는 다음과 같은 측면에서 긍정적인 영향을 발휘하고 있다.

- 브랜드 평판
- 고객 및 디지털 신뢰
- 운영 안정성(공급망, 파트너사 생태계 포함)
- 매출

또한 사이버 성숙도가 높은 기업들은 사이버가 주요 사업 전략에 가치를 창출하며 새로운 것을 시도할 수 있는 자신감을 주고 비즈니스 민첩성을 높이며 효율성을 가져온다고 응답했다. 그리고 성숙도가 높은 기업들은 이들이 활용하고 있는 제3자 사이버 서비스의 가치를 매우 높게 산다고 보고하는 경향이 더 크다.

비즈니스의 발전

"프로젝트, 이니셔티브, 사업 목표는 정보 보안과 개인정보 보호에 대한 영향을 고려하지 않고는 달성할 수 없습니다. 또한 적절한 프로세스에 이를 적용하지 않고는 달성할 수 없습니다. 저희는 아이디어 구상 단계에서부터 관여하기 시작합니다. 사이버가 사업 구성요소와 영역에 연관되어 있기 때문입니다. 저희의 전략은 사업을 지원하는 데 100% 포커스가 맞춰져 있습니다. 사이버와 개인 정보 보호는 사업 없이는 존재할 수 없다는 것을 알기 때문이죠. 저희는 법을 준수하고 안전한 선에서 사업을 발전시키고 성장을 촉진하는 데 의미 있는 기여를 하고 싶습니다."

메리어트(Marriot)사 SVP & CISO, 아르노 밴 더 월트

사이버는
'비즈니스를 가능하게 하는 요소',
즉 비즈니스 인에이블러
(business enabler)로서의
잠재력이 있으나,
사이버를 효과적으로 활용할 수
있는 능력은 기업마다
천차만별일 수 있다.
일부 기업들은 다른 기업들이
벤치마킹할 수 있는 선두 주자로
부상했다.

54%

미화 50억 달러 이상의 수익을 올리는 기업 중 54%가 사이버와 관련해 2억 5천만 달러 이상을 지출하고 있다

71%

미화 5억 달러에서 50억 달러 사이의 수익을 올리는 기업 중 71%가 사이버와 관련해 2억 5천만 달러 이하를 지출하고 있다

방법론

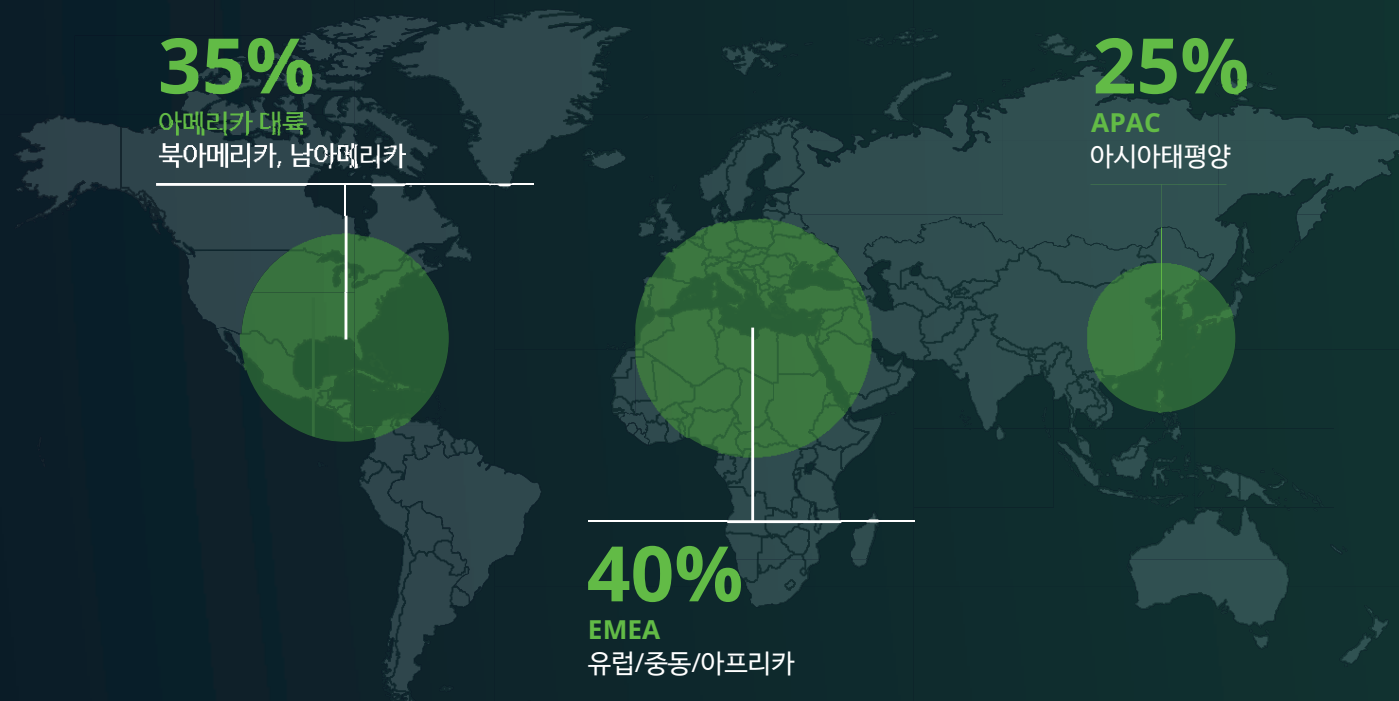
딜로이트는 오늘날 복잡한 사업 환경과 기술 환경을 바탕으로 '사이버의 미래 2023 서베이'를 고안했다. 본 조사는 사이버의 중요성을 인식하며 그 가치를 제대로 활용하기 위해 고군분투하는 기업 리더의 니즈에 초점을 맞췄다. 딜로이트는 20개국의 이사 직급 이상의 사이버 관련 의사 결정권자 1,000명 이상을 대상으로 설문조사를 실시했다. 조사 대상 기업은 직원 수가 최소 1,000명 이상이고 연간 수익이 미화 5억 달러에 달하는 기업으로 제한했다.

오늘날 사이버가 기업에 미치는 영향을 정확하게 파악하기 위해, 지난 2021년 연구에서 약 600명이었던 표본 크기를 올해는 1,110명으로 거의 두 배가량 늘렸다. 딜로이트는 또한 다양한 산업과 지역의 사이버 관련 고위 의사 결정권자들과 심층 인터뷰를 실시하여 보다 자세한 인사이트를 얻고 관찰 결과를 검증했다. 본 연구의 접근법은 전략에서부터 구체적인 방안과 문화, 기술 구현에 이르기까지 사이버의 미래와 관련된 모든 측면을 다루었다.

본 연구는 다음에 집중하였다.

- 지난 2021년 서베이 이후 사이버 분야가 어떻게 변화했는지 파악
- 미래의 사이버 환경을 보다 명확히 파악할 수 있도록 미래 지향적인 관점 사용
- 기업이 경험하고 있는 사이버의 비즈니스 가치와 영향에 대해 이해하고, 선도 기업이 사이버를 통해 더 많은 가치를 얻기 위해 취하고 있는 조치에 대해 이해

조사 대상 기업의 본사 위치



미래는 사이버다

본 연구는 지난 2년 동안 사이버가 어떻게 발전해 왔는지 설명하는 데서 나아가, 선도 기업이 성숙한 사이버 전략을 채택할 때 비즈니스에 미치는 영향에 대해 이해하기 위해 '사이버 성숙도'(cyber maturity)에 대한 견해를 발전시켰다.

성숙도가 높은 기업과 중간 수준 및 낮은 수준의 성숙도를 구분해서 보면 사이버 분야의 선두 주자들을 파악할 수 있고 사이버가 어느 정도로 사업의 성공과 가치를 뒷받침하는지 더 완전하게 이해할 수 있다.

오늘날 사이버는 비즈니스와 직결된다. 사이버는 비즈니스의 기반이자 필수 요소이다. 어떤 기업이든 사이버의 성공 여부는 최고 경영진 및 이사회의 의지, 그리고 사이버를 통해 구상하는 비즈니스 가치에 의해 좌지우지될 것이다. 본 연구 결과는 정보보호 최고책임자(CISO)와 기타 C레벨 임원진이 이사회와 더불어 비즈니스를 이끌고 혁신을 실현하기 위해 협력함에 따라, 새로운 다이나믹이 나타나고 있음을 보여준다. 다시 말해 사이버는 광범위한 비즈니스 전략에 내재되어야 한다. 단순히 IT 관련 리스크를 완화하는데 그치는 것이 아니라 지속적인 비즈니스 가치를 창출하기 위한 성공의 필수 요소로서 모든 부서 영역에 포함되어야 한다.

영향력 입증

"리스크를 최소화할 때 우리는 어디서 어떻게 영향을 미쳤는지, 운영을 원활하고 효과적인 방식으로 지속할 수 있었는지를 명확히 알 수 있습니다. 특히 많은 경우 운영 및 통합 문제가 있었던 비즈니스 파트너와 비교할 때 그렇습니다."

소비재 기업 CISO

사이버의 발전 현황

2021년 마지막 분기에 서베이 보고서가 나온 이후, 전 세계 산업들은 다양한 영역에서 지속되는 격변을 헤쳐 나가는 동시에 이에 맞춰 우선순위와 비즈니스 이니셔티브, 역량을 그에 맞게 조정했다.

2021년 서베이와 금번 서베이 모두 응답자들에게 기업에 중요한 기술, 따라서 미래 사이버 전략에서 고려해야 할 기술을 파악하기 위해 기업의 디지털 전환 우선순위에 대해 질문했다.

2021년 순위와 비교하자면, 클라우드가 데이터 애널리틱스를 제치고 2위에서 1위로 올라갔다. 운영기술(OT) 및 산업용제어시스템(ICS)과 인공지능/인지 컴퓨팅이 소폭 상승하며 5위권에 여전히 자리를 지키고 있다. 올해에는 5G가 처음으로 5위권에 진입했다. 기업들의 비즈니스 목표에서 5G의 역할이 커지고 있음을 알 수 있다.

클라우드는 계속해서 중요한 기술로 자리매김하고 있다. 이로 인해 데이터와 애플리케이션을 오프프레미스(off-premise)로 다양한 환경에서 호스팅하는 데서 오는 복잡한 고려 사항들이 생긴다. 클라우드의 성숙도는 제각기 다르지만 최신 사이버의 미래 서베이 연구 결과에 따르면 많은 기업들이 이러한 우려를 극복하고 있으며 리스크 관련 클라우드 사용 사례에서 매우 긍정적인 결과를 얻고 있는 것으로 나타났다. 실제로 기업의 83%가 클라우드 투자가 비즈니스 및 규제 리스크를 완화하는 데 있어 긍정적인 결과를 낳고 있다고 답했다[2]. 이는 성숙한 사이버 클라우드 역량, 공동 책임 모델(shared responsibility model), 개인 정보 보호 프로그램과 관련해 긍정적인 신호이다.

디지털 전환 우선순위

사이버의 역할

서베이의 일환으로 이러한 주요 디지털 전환 이니셔티브에서 사이버의 역할에 대해 물었다. 경영진은 모든 디지털 전환 이니셔티브에서 사이버가 중요한 역할을 한다고 봤으며, 특히 클라우드, 데이터 애널리틱스, 5G분야에서 더욱 그렇다고 봤다(그림 1).

주요 디지털 기술과 신흥 기술이 진화했지만 사이버 사고가 조사 대상 기업에 미치는 영향 또한 진화했다. 기업들은 잘 갖춘 사이버가 가져올 수 있는 긍정적인 이점과 장기적인 사업 가치에 초점을 맞추면서 동시에 사이버 위협에 대응하여 부정적인 비즈니스 결과와 리스크를 완화하는 사이버의 핵심 능력 또한 놓치지 않는 것이 중요하다.

최우선 과제, 사이버

"모두가 사이버를 최우선 의제로 삼고 있으며, 전략과 예산, 솔루션을 고안할 때 사이버를 포함하고 있습니다."

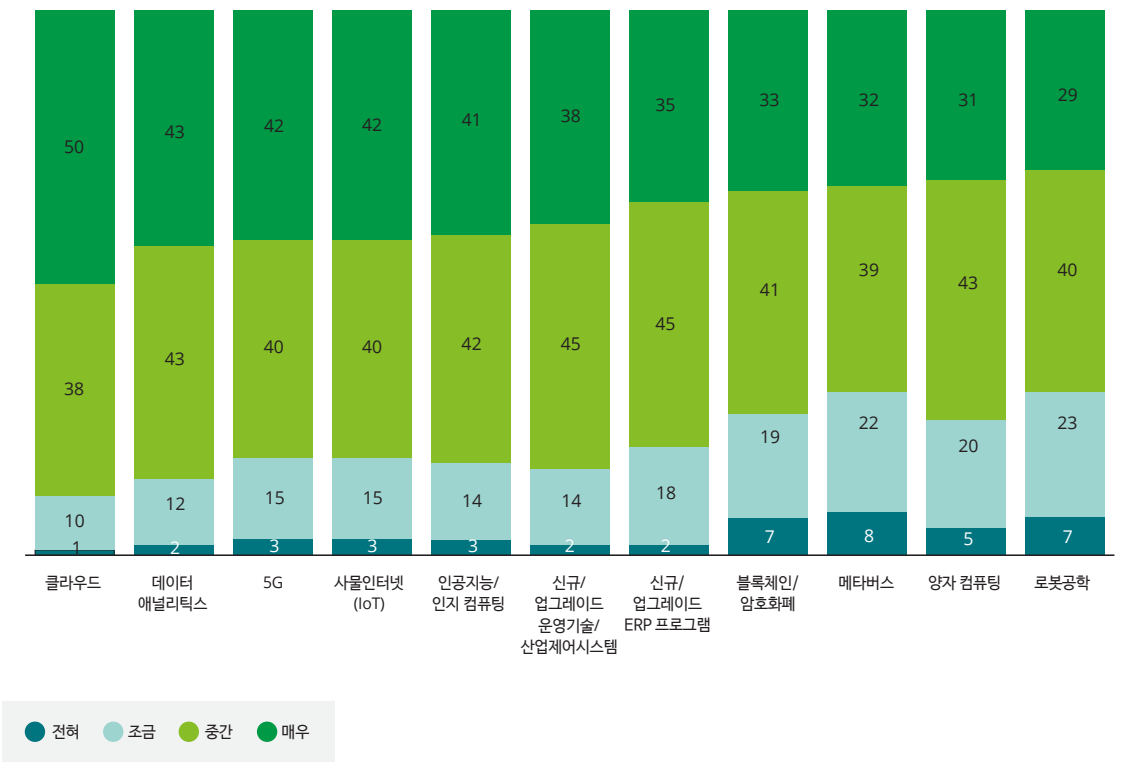
금융서비스 기업 CISO

그림 1. 주목받는 사이버

질문: 사이버가 기업의 디지털 전환 이니셔티브에서 주도적인 역할을 할 것으로 기대한다

(반올림으로 인해 백분율 수치의 합이 100%가 아닐 수 있음)

(단위: %)



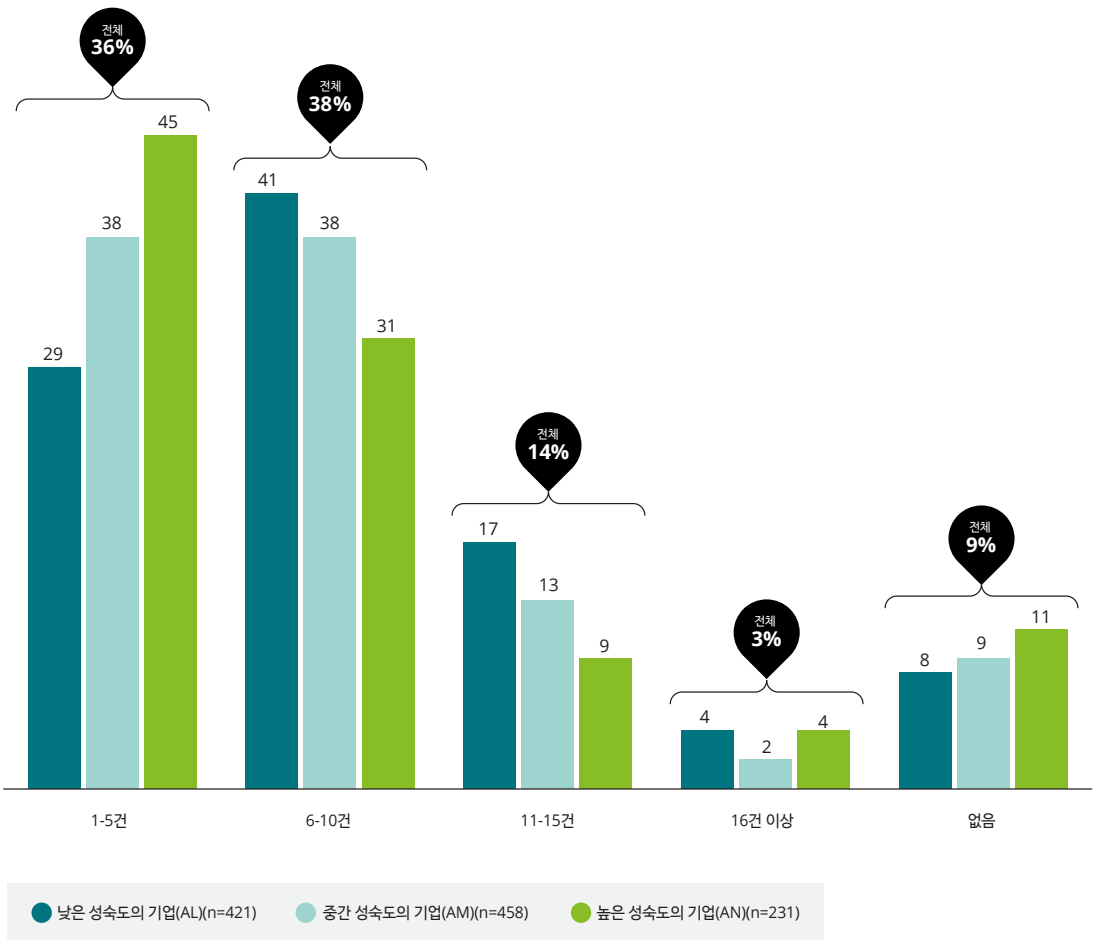
사이버 사고와 그 영향에 대한 인사이트

사이버 사고나 위반의 빈도수에 대해 최소 1건을 보고한 기업이 2021년 조사에서는 88%, 올해 조사에서는 91%로 꾸준히 유지되는 중이다. 수많은 행위자, 출처, 도구, 테크닉 등이 기업들이 우려하는 사이버 문제에 포함된다. 성숙도가 높은 기업들은 피싱이나 악성 프로그램, 랜섬웨어 공격뿐만 아니라 사이버 범죄자와 테러리스트에 대해 우려하고 있는 것으로 보인다. 성숙도가 낮거나 중간 수준인 기업들은 서비스 거부(DoS) 공격에 대한 우려가 크다. 성숙도가 낮은 기업이 중대한 사이버 보안 사고를 더 많이 경험한다고 응답한 사실은 주목할 만하다(그림 2).

91%

한 건 이상의 사이버 사고 또는 위반을 보고한 기업

그림 2. 중대한 사이버 보안 사고 건수(%)



한편 사이버 사고로 인한 가장 큰 부정적 결과는 여전히 운영상 차질인 것으로 나타났으며, 매출 손실과 고객 신뢰 상실이 각각 2위와 3위로 뛰어올랐다. 56%의 응답자가 이에 관련한 결과를 중간 수준 또는 상당한 수준으로 겪었다고 응답했다. 이 부분에서 한 가지 가설이 작용하고 있을 수 있다. 높은 수준의 성숙도를 보이는 기업들이 비즈니스에서 실제로 어떤 일이 일어나고 있는지 심층적으로 이해하기 때문에 사이버 사고의 영향을 더 명확히 파악할 수 있다. 성숙도가 낮은 기업은 이론적인 영향만 평가할 수 있을 것이다.

성숙도가 높은 기업이 사이버 이니셔티브로부터 얻는 이익은 더욱 명확하다. 이들 기업은 브랜드 평판, 신뢰도, 운영 및 재무 등 여러 부문에서 개선 효과를 얻었다. 반면 성숙도가 낮거나 중간 수준인 집단에서는 브랜드 평판과 신뢰도 정도만 개선된 것으로 나타났다.

이러한 맥락에서 봤을 때, 사이버 전략, 솔루션, 컨트롤로 이뤄진 기업의 생태계 전반에 걸쳐 리스크를 중심으로 하는 사이버 전략의 필요성은 사이버의 미래를 위해 그 어느 때보다 중요하다. 제로 트러스트(zero trust) 아키텍처는 보안 상태를 강화하고 보안 관리를 단순화하며 최종사용자 경험을 개선하여 최첨단 엔터프라이즈 환경을 실현할 수 있다. 제로 트러스트로 나아가기 위해서는 비즈니스 성과에 부합하는 전략과 계획이 필요하며 상당한 노력을 요한다. 여기에는 기초적인 사이버 이슈 해결, 수동 프로세스의 자동화, 보안 조직과 기술 환경은 물론 기업 자체에 혁신적인 변화를 불러오는 계획 등이 포함된다[3].

제로 트러스트 구현

제로 트러스트를 구현하는 것은 단순히 기술을 구현하는 것이 아니다. 문화와 커뮤니케이션 방식과 인식이 바뀌는 사업적, 문화적 변화이기도 하다.

포괄적인 제로 트러스트를 구현하려면, 거버넌스(아키텍처 및 운영), 애널리틱스 및 자동화 등의 인에이블러, ID와 데이터, 장치 등의 핵심 영역을 포함해 여러 요소를 다뤄야 한다.

그림 3. 사이버 사고와 위반이 초래하는 부정적인 결과

사이버 사고 및 위반의 부정적 결과	2021(순위)	2023(순위)	2023(비율)
운영상 차질(공급망/파트너 생태계 포함)	1	1	58%
매출 손실	9	2	56%
고객 신뢰 상실/브랜드에 부정적 영향	4	3	56%
평판 저하	5	4	55%
전략적 이니셔티브에 대한 자금 철회	N/A	5	55%
기술 무결성에 대한 신뢰 상실	N/A	6	55%
인재 채용/유지에 미치는 부정적 영향	8	7	54%
지적 재산권 침해	2	8	54%
주가 하락	3	9	52%
규제 과태료	7	10	52%
리더십 변화	5	N/A	N/A

56%의

응답자가 매출 손실 및 고객 신뢰 상실을 중간 수준 또는 상당한 수준으로 겪었다고 응답

사이버 성숙도 평가 기준

사이버의 중요성이 점차 높아지고 있는 가운데, 전 세계 수천 개 기업과 협업한 경험을 바탕으로 응답자들을 당사의 사이버 성숙도에 따라 세분화했다.

사이버 성숙도의 정의

'사이버 성숙도'를 정의하며 사이버의 미래를 그려 나가고 있는 성숙도가 높은 기업을 파악하고자, 세 가지 주요 관행을 기준으로 기업들을 평가했다.

사이버 위협에 방어하고 대응하기 위한 전략, 운영, 전술 계획의 유무로 알 수 있는
탄탄한 사이버 계획

정성적 및 정량적 리스크 평가, 업계 벤치마킹, 사고대응 시나리오 계획 등
주요 사이버 활동

이사회가 정기적으로 사이버 관련 이슈를 다루는지 여부로 알 수 있는
이사회의 실질적 참여

사이버 성숙도 그룹 자세히 살펴보기

각 주요 관행에 대한 점수를 매김으로써 조사 대상 기업을 세 그룹으로 분류할 수 있었다.

38%

사이버 성숙도가 낮은 기업

어떤 주요 관행도 실천하지 않음

41%

사이버 성숙도가 중간인 기업

주요 관행 중 한 가지 실천

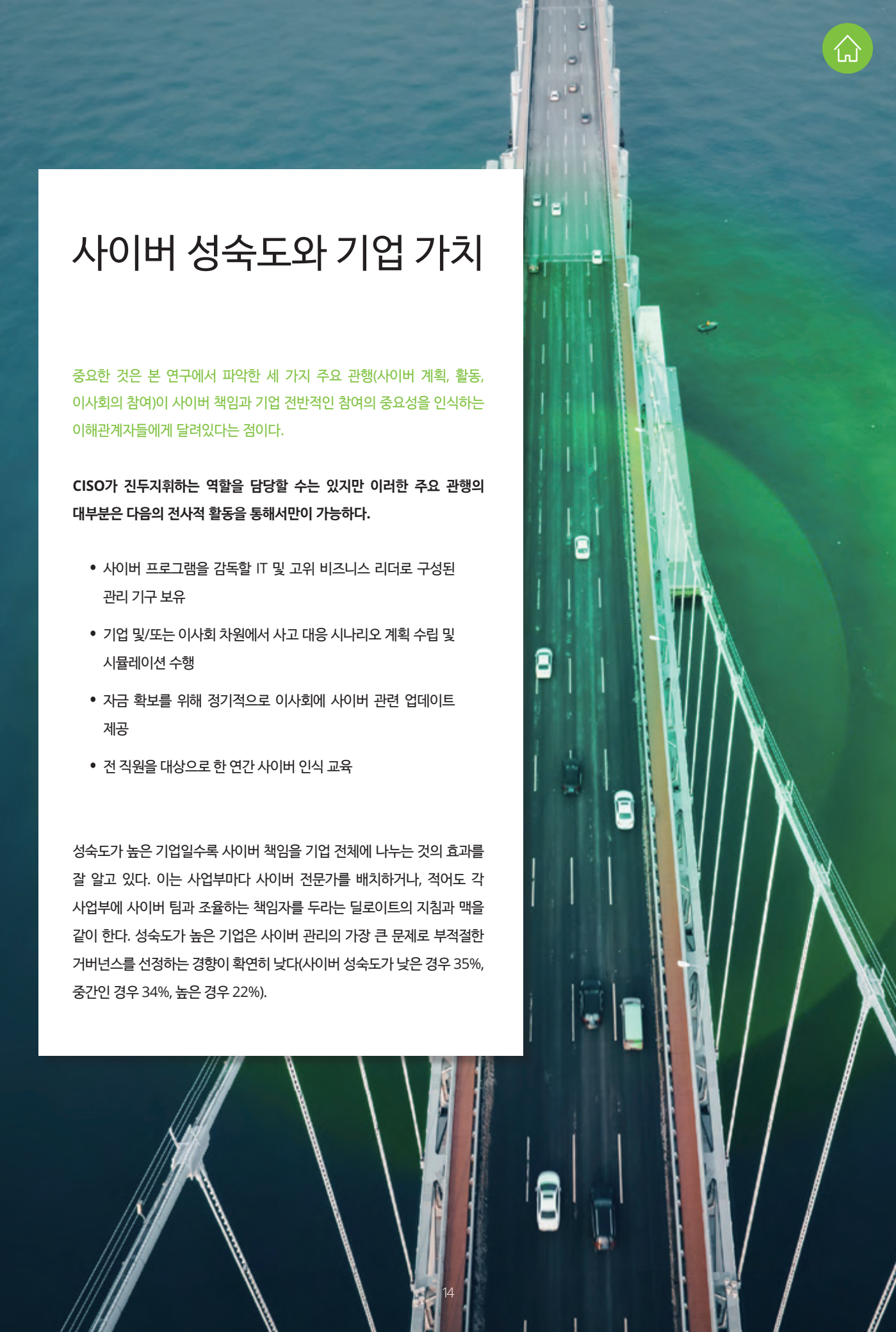
21%

사이버 성숙도가 높은 기업

주요 관행 중 두세 가지 실천

사이버 성숙도와 규모/산업의 상관관계

세 그룹을 살펴보면서 성숙도에 따른 경향이나 특성을 파악하기 위해 기업들의 일반적인 특성도 파헤쳤다. 각 그룹에 속한 기업은 다양한 산업에 속해있었으며, 기업 규모나 매출액도 사이버 성숙도와 상관관계가 없는 것으로 나타났다. 이를 통해 성숙도는 산업이나 기업 규모에 크게 좌우되지 않을 수 있음을 알 수 있다.



사이버 성숙도와 기업 가치

중요한 것은 본 연구에서 파악한 세 가지 주요 관행(사이버 계획, 활동, 이사회의 참여)이 사이버 책임과 기업 전반적인 참여의 중요성을 인식하는 이해관계자들에게 달려있다는 점이다.

CISO가 진두지휘하는 역할을 담당할 수는 있지만 이러한 주요 관행의 대부분은 다음의 전사적 활동을 통해서만이 가능하다.

- 사이버 프로그램을 감독할 IT 및 고위 비즈니스 리더로 구성된 관리 기구 보유
- 기업 및/또는 이사회 차원에서 사고 대응 시나리오 계획 수립 및 시뮬레이션 수행
- 자금 확보를 위해 정기적으로 이사회에 사이버 관련 업데이트 제공
- 전 직원을 대상으로 한 연간 사이버 인식 교육

성숙도가 높은 기업일수록 사이버 책임을 기업 전체에 나누는 것의 효과를 잘 알고 있다. 이는 사업부마다 사이버 전문가를 배치하거나, 적어도 각 사업부에 사이버 팀과 조율하는 책임자를 두라는 딜로이트의 지침과 맥을 같이 한다. 성숙도가 높은 기업은 사이버 관리의 가장 큰 문제로 부적절한 거버넌스를 선정하는 경향이 확연히 낮다(사이버 성숙도가 낮은 경우 35%, 중간인 경우 34%, 높은 경우 22%).

그림 4. 산업별 사이버 활동 진척 상황

사이버 활동 예시

- 매년 사이버 계획 분석 및 업데이트
- 사이버 프로그램을 감독할 고위 비즈니스 및 IT 리더로 구성된 관리 기구 보유
- 리스크 정량화 도구를 사용하여 사이버 투자에 따른 수익률 측정 및 확보
- 기업 및/또는 이사회 차원에서 사고 대응 시나리오 계획 수립
- 사이버 이니셔티브를 관리하기 위한 외부 도움/아웃소싱 확보

사이버 계획 전략 예시

- 전 직원을 대상으로 하는 연간 사이버 인식 교육
- 매년 사이버 사고 대응 계획 업데이트 및 테스트
- 데이터가 어디에 저장, 처리, 전송되는지 관련하여 각 단계마다 데이터 보호 방식을 평가하는 포괄적인 계획
- 파트너와 공급업체의 보안 상태를 모니터링 및 추적하는 사이버 리스크 프로그램
- 사이버 및 개인 정보 보호 요구사항에 대한 지속적인 고객 의견 수렴

산업

본 연구에 포함된 6개 산업 중 3개 산업('정부 및 공공 부문', '에너지, 자원 및 산업재 부문', '첨단기술, 미디어 및 통신 부문')은 5개 이상의 사이버 활동을 시행하고 있는데 이는 전체 평균보다 약간 높은 수치이다.

두 개 산업('에너지, 자원 및 산업재 부문', '생명과학 및 헬스케어 부문')은 전체 평균보다 약간 더 높은 수준으로 5개 이상의 사이버 계획 전략을 구현하고 있다.

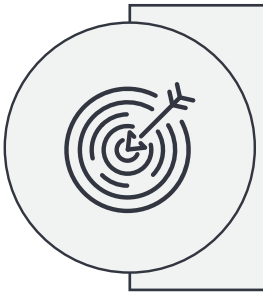
한편 금융 부문은 8개 사이버 계획 전략 중 4개 전략을 평균보다 약간 더 높은 수준으로 시행하고 있다. 그러나 이 산업은 사이버 활동에 있어서는 전체 평균보다 뒤처져 있으며, 한 개의 활동에서만 전체 평균보다 높은 수준이다.

그리고 본 연구의 데이터에 따르면 소비자 부문이 다른 산업들보다 약간 뒤처져 있는데 10개의 핵심 사이버 활동 중 7개는 전체 평균보다 약간 뒤처져 있고 8개 사이버 계획 전략이 모두 전체 평균보다 낮은 수준으로 실행되고 있다.

기업 규모

본 연구 결과에 따르면 20,000명 이상의 직원을 둔 기업들에 대해 다음과 같은 경향이 더 높다고 밝혔다.

- 리스크 관리, 디지털 전환, 디지털 신뢰, 기술 현대화와 관련된 비즈니스 전략의 중요성을 이해
- 이러한 비즈니스 전략에서 사이버의 중요성을 인지
- 사이버 계획 및 주요 사이버 활동을 진행할 경향이 높음



핵심

산업이나 규모에 관계없이 어떤 기업이든 사이버와 관련해 높은 성과를 거둘 수 있으며 성숙도가 높은 방향으로 나아갈 수 있다. 성공 여부는 사이버에 대한 투자를 늘려 성숙도를 '구매하는' 능력에만 달려있지 않다. 오히려 기업들이 취하는 행동과 구축하는 문화가 성과를 향상하는 주요 요소가 될 것이다.

*본 서베이에서 '소기업'은 매출액이 미화 5억 달러에서 10억 달러에 이르는 기업을 가리킨다.
'대기업'은 미화 100억 달러 이상의 매출을 올리는 기업을 가리킨다.

사이버를 통한 비즈니스 성장

가치를 창출하는 사이버 투자

절대적인 보안과 리스크 완화를 보장할 수 있는 사이버 아키텍처나 접근법은 없다. 기업이 얼마나 성숙하든 상관없다. 대신 사이버 성숙도가 높은 기업의 가장 두드러진 특징은 바로 사이버 투자에서 가치를 창출할 수 있다는 점이다.

성숙도가 높은 기업들은 리더십의 참여도가 높으며 심사숙고하여 계획을 세우고 행동으로 옮긴다. 그리고 사이버에 대한 이들의 노력은 더 많은 비즈니스 가치로 결실을 맺고 있는 것으로 보인다. 성숙도가 높은 기업들은 효율성과 회복 탄력성, 민첩성 향상 등의 측면에서 선두를 차지하고 있으며, 일반적으로 사이버와 연관이 있다고 쉽게 생각하지 못하는 이점들을 파악하고 있다.

높은 사이버 성숙도의 긍정적 영향

이렇게 성숙도가 높은 기업 중 절반 이상(55%)은 사이버가 새로운 것을 시도할 수 있는 자신감을 준다고 답했는데, 이에 비해 같은 응답을 한 중간 성숙도 기업은 45%, 낮은 성숙도 기업은 40%였다.

그리고 성숙도가 높은 기업 중 약 70%는 사이버가 신뢰도 및 효율성 개선에 모두 영향을 미치고 있다고 응답했다. 이는 성숙도가 낮거나 중간 수준인 기업에 비해 상당히 높은 수치이다.

마찬가지로 성숙도가 높은 기업의 과반수(65%)가 사이버의 긍정적 영향으로 회복탄력성과 민첩성을 꼽았는데, 이 또한 성숙도가 낮거나 중간 수준인 기업을 크게 앞선 수치이다(그림 5).

55%

성숙도가 높은 기업 중 절반 이상은 사이버가 새로운 것을 시도할 수 있는 자신감을 준다고 응답

그림 5. 사이버가 긍정적 영향을 미치는 비즈니스 이니셔티브

(단위: %)

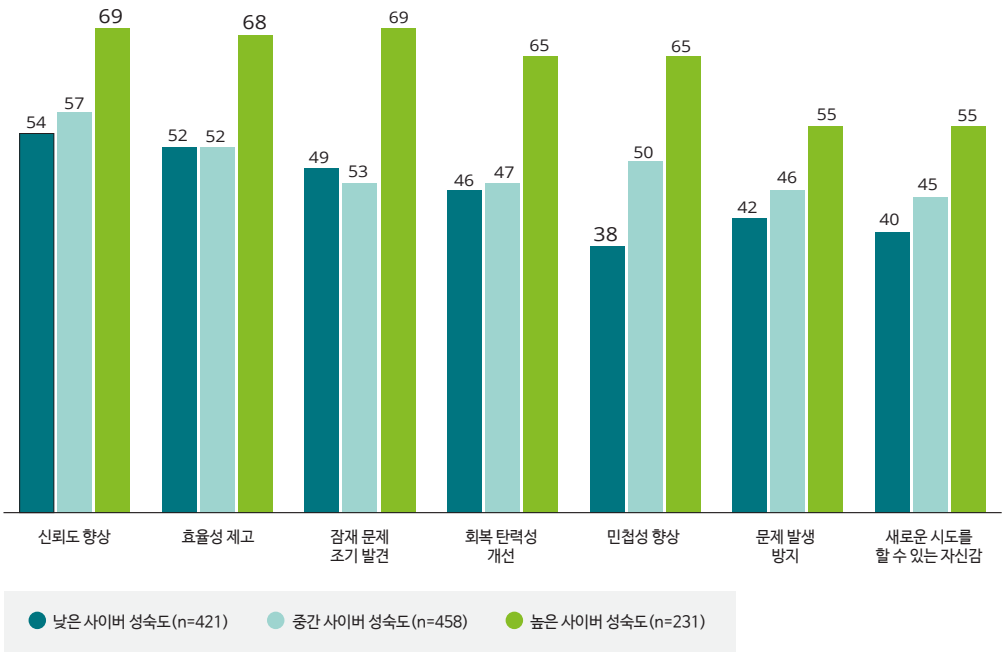
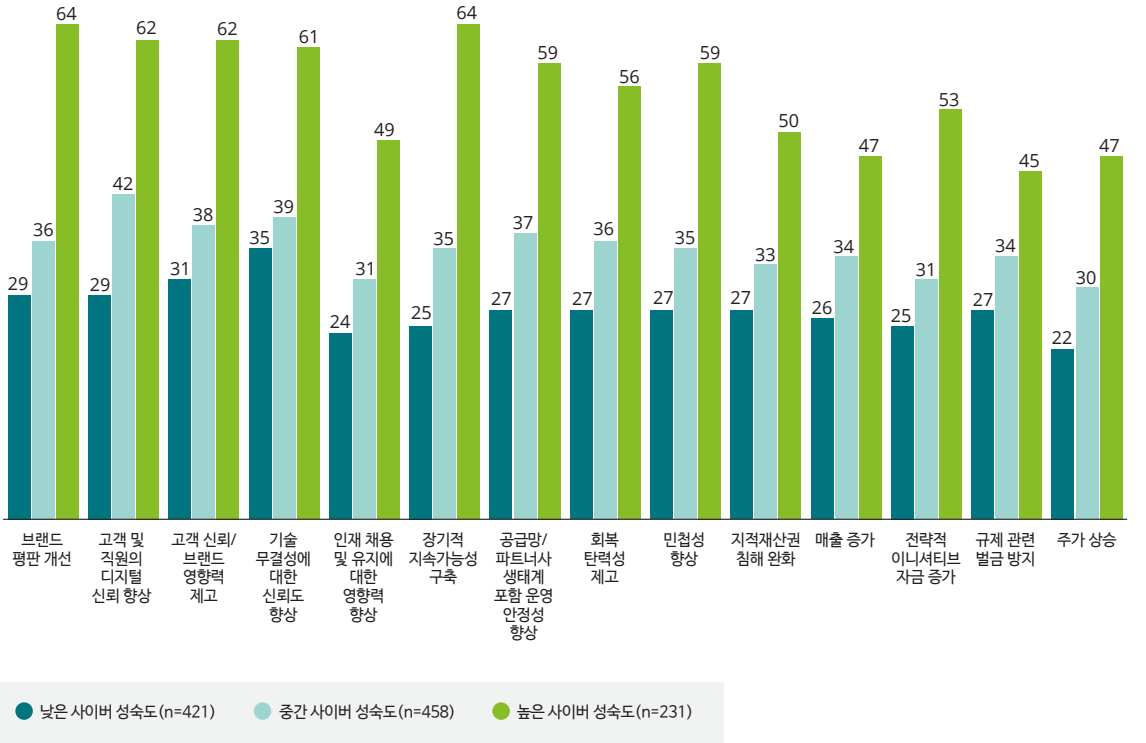


그림 6. 사이버 이니셔티브가 긍정적으로 기여하는 영역

(단위: %)



또한 성숙도가 높은 기업들은 브랜드 평판 향상(64%), 매출 증가(47%), 공급망 및 파트너사 생태계 관련 운영 안정성 향상(59%), 인재 채용 및 유지(49%), 장기적 지속가능성 구축(64%), 고객 신뢰 및 브랜드 영향력 제고(62%) 등의 영역에서 사이버 이니셔티브에 기인한 긍정적인 영향을 보고하는 경향이 더 높다.

신뢰는 사이버에 있어 가장 중요한 문제이다. 성과를 내는 데 도움이 될 수 있는 생태계인 이해 관계자들과 신뢰 관계를 구축해야 한다. 예를 들어 기업을 신뢰하는 직원은 고객 만족도를 2배나 향상시키고 브랜드를 신뢰하는 고객은 재구매하는 경향이 88% 더 높다[4]. 고객과의 신뢰 구축은 또한 파트너사에게도 영향을 미치고 시가총액을 최대 4배까지 향상시키며, 신뢰받는 회사들은 궁극적으로 동종업체보다 최대 400% 더 좋은 성과를 낸다[5].

그리고 '사이버의 미래 2023 서베이' 결과 자료를 통해 글로벌 기업 사이에서 사이버 성숙도가 신뢰 등을 포함한 이점으로 어떻게 이어지는지 연관성을 확인할 수 있다. 사이버에 투자하는 기업들은 다양한 가치 척도로 봤을 때 상당한 이득을 보고 있으며 사이버 성숙도가 높은 기업은 모든 전략적 척도에서 더 많은 가치를 얻고 있다(그림 6).

고객의 기대

"개인적인 생각으로는 고객들이 사이버 보안 때문에 당사 제품에 많은 추가 비용을 지불할 의사는 없을 것으로 봅니다. 그래도 고객은 사이버 보안을 기대할 거예요. 사이버 보안은 차별화 요소가 될 것입니다."

자동차 기업 CISO

400%

고객 신뢰 구축은 파트너사에 영향을 미치고 시가총액을 400% 증가시키며 신뢰받는 기업은 궁극적으로 동종업체보다 최대 400% 더 좋은 성과 창출

사이버 성숙도가 높은 기업이 중하위 그룹의 기업을 능가하는 또 다른 영역은 외부 사이버 서비스를 통해 얻는 가치이다.

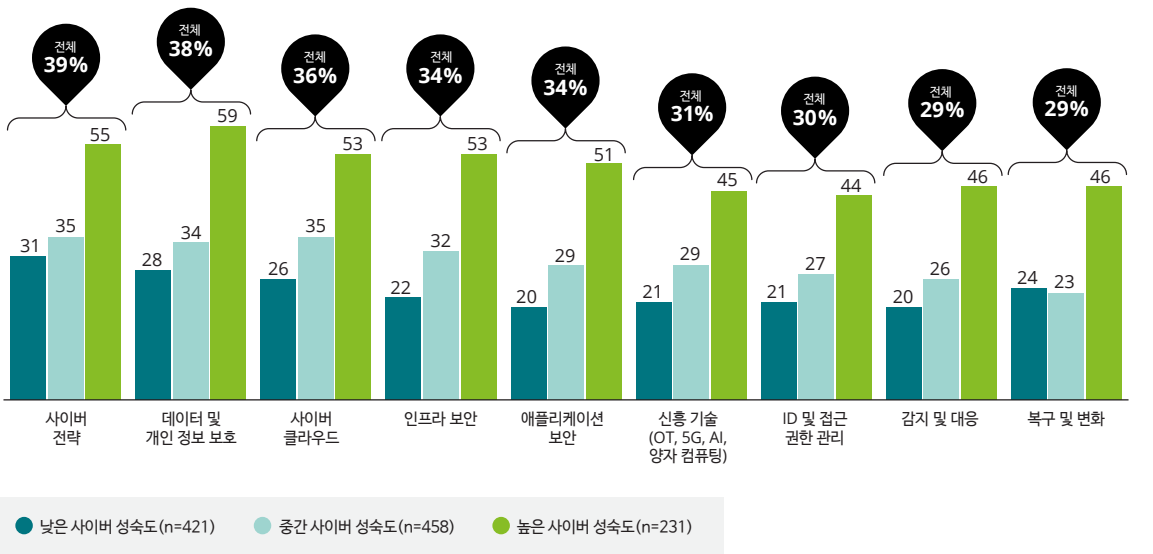
성숙도가 높은 기업의 대다수는 사이버 전략, 데이터 및 개인 정보 보호, 사이버 클라우드, 인프라 보안, 애플리케이션 보안과 관련한 외부 서비스에 대해 상당한 가치를 얻는다고 보고했다. 한편 소수의 중하위 기업만이 이러한 영역에서 가치를 얻는다고 보고했다.

기업들이 외부 사이버 서비스가 가져올 수 있는 가치를 얻기 위해서는 커져가는 서비스 생태계와 고유의 복잡성을 관리할 수 있는 방안에 대해 고려해야 한다(그림 7).

그림 7. 공급 업체를 통한 가치 실현

기업이 외부 사이버 서비스를 통한 가치 창출을 보고하는 경우

(단위: %)



교훈
선도 기업 벤치마킹

성숙도가 높은 기업이 사이버 투자로 상당한 비즈니스 효과를 얻을 수 있다는 점을 감안하면, 다른 기업들은 성숙한 사이버 기업의 사례를 참고하여 이를 기업 차원의 폭넓은 사이버 참여를 달성하기 위한 가이드로 활용해야 한다.

성숙도가 높은 기업이 사이버로부터 얻은 성공을 바탕으로 기업에서는 다음과 같은 질문에 대해 더 깊이 연구해 볼 수 있다.

- 적합한 기술과 파트너사 생태계를 보유하고 있는가? 커져가는 복잡한 제3자 네트워크를 어떻게 관리할 수 있는가?
- 적절한 방안과 적절한 영역에 투자하고 있는가? 또한 기업 전체에 걸쳐 사이버가 어디에서, 어떻게 가치를 더하고 있는지 이해하기 위한 적절한 프레임워크가 마련되어 있는가?
- 기업 전체에 걸쳐 사이버가 어디에서, 어떻게 가치를 더하고 있는지 이해하기 위한 적절한 "가치 프레임"이 마련되어 있는가?

사이버의 미래를 좌우하는 주요 통찰력

1. 다각적인 활동

앞서 언급했듯 사이버 성숙도가 높은 기업은 사이버 활동을 위해 기업 전체가 움직인다. 성숙도가 높은 기업은 성숙도가 중간이거나 낮은 기업보다 모범 사례를 더 많이 실행하는데, 기업 차원의 활동량에 있어서 그 차이가 가장 극명하게 나타난다.

리더십. 성숙도가 높은 기업은 고위 비즈니스 및 IT 리더로 구성된 관리 기구를 보유하여 성숙도가 낮은 기업에 비해 사이버 프로그램을 감독하는 경향이 3배가량 높으며, 중간 수준의 기업에 비해서는 2배가량 높다(성숙도 높은 기업 60%, 중간 기업 36%, 낮은 기업 22%).

시나리오 계획. 마찬가지로 성숙도가 높은 기업은 기업 차원 및/또는 이사회 차원에서 사건 대응 시나리오 계획을 수립하는 경향이 낮은 성숙도의 기업보다 3배 높으며 중간 수준의 기업보다 2배 높다(성숙도 높은 기업 60%, 중간 기업 30%, 낮은 기업 20%).

2. 디지털 전환 이니셔티브에서 사이버의 중요도

성숙도가 높은 기업들은 사이버를 디지털 전환을 위한 주요 이니셔티브의 핵심으로 평가하는 경향이 훨씬 크다(그림 8).

이러한 디지털 전환 이니셔티브를 채택하는 것은 운영 민첩성과 비즈니스 성공을 보장하는 데 필수적이다. 그러나 각 이니셔티브는 상당한 사이버 리스크를 수반하며 성숙도가 높은 기업은 이 사실을 이미 잘 알고 있다.

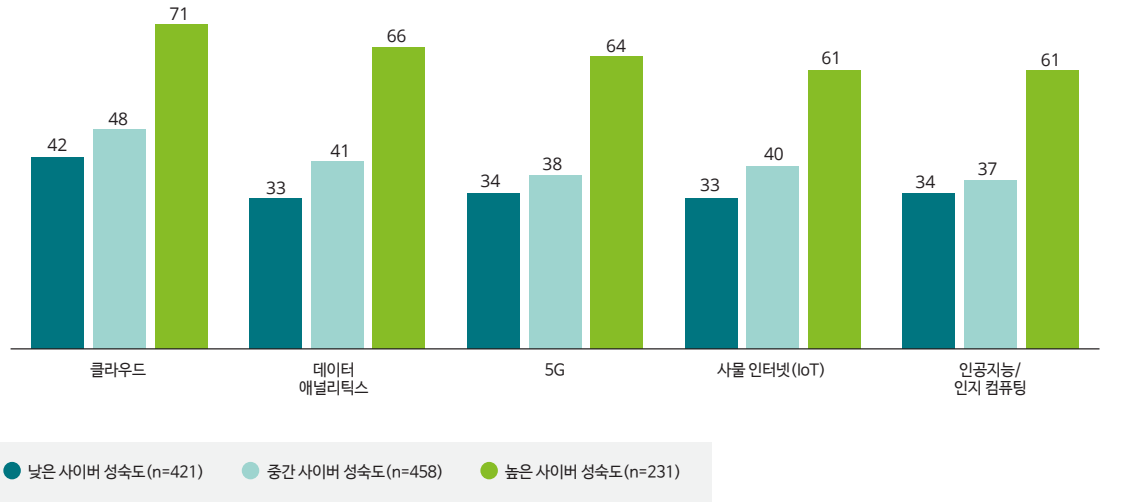
예를 들어 AI는 사이버 전략과 기업의 디지털 사업 목표를 가능케 할 수 있지만 잠재적인 사이버 리스크를 가져오기도 한다. 어떤 디지털 기술이라도 마찬가지이다. 앞서 다룬 모범 사례 외에도, 딜로이트의 또 다른 최신 서베이(State of AI in the Enterprise) 또한 리스크 완화 조치를 취하는 것이 비용 절감과 새로운 시장 진출 등 더 나은 결과를 이끌어내는 데 어떻게 도움이 될 수 있는지를 조명한다. AI와 관련된 리스크는 기업에 매우 중요한 전형적인 이슈이다. 해당 서베이에 따르면 AI 의사 결정의 설명 가능성(explainability)과 투명성(transparency), 개인 정보 보호/동의에 대한 관리 부실, AI 시스템의 안전 우려가 모든 기업들이 우려하는 윤리 리스크만큼이나 크게 나타나고 있다[6].

이러한 리스크를 관리하는 것은 기업의 AI 관련 활동에 큰 영향을 미칠 수 있다. 실제로 이번 AI 조사에서 응답자의 50%가 AI 프로젝트 규모를 확대하는 데 가장 큰 걸림돌로 AI 관련 리스크 관리를 꼽았다. 이러한 분위기에도 불구하고 응답자의 33%만이 AI 리스크 관리를 기업의 리스크 관리 활동에 포함했다. 성숙도가 높은 기업의 33%와 낮은 기업의 29%가 외부 업체와 협력하여 AI 시스템을 독립적으로 감사하고 있다.

그림 8. 사이버와 함께 하는 발전

각 성숙도 그룹별 각 디지털 전환 이니셔티브가 중요하다고 응답한 비중

(단위: %)



3. 탄탄한 계획 수립

'계획'은 리스크를 효과적으로 완화하고 비즈니스 가치를 창출하는 사이버 전략을 수립하는 데 가장 중요한 요소이다. 그리고 본 연구에 응답한 성숙도가 높은 기업은 계획의 필요성을 충분히 인식하고 있는 것으로 보인다(그림 9).

사이버 성숙도가 높은 기업은 다음과 같은 요소를 포함하여 강력한 계획을 수립하는 경향이 크다.

- 사이버 보안 사고 대응 계획에 대한 연간 업데이트 및 테스트(성숙도 높은 기업 87%)
- 사이버 위협으로부터 방어하기 위한 운영 및 전략 계획 (91%)
- 데이터가 저장, 처리, 전송되는 각 단계마다 데이터를 어떻게 보호하는지 평가하는 포괄적인 계획(88%)

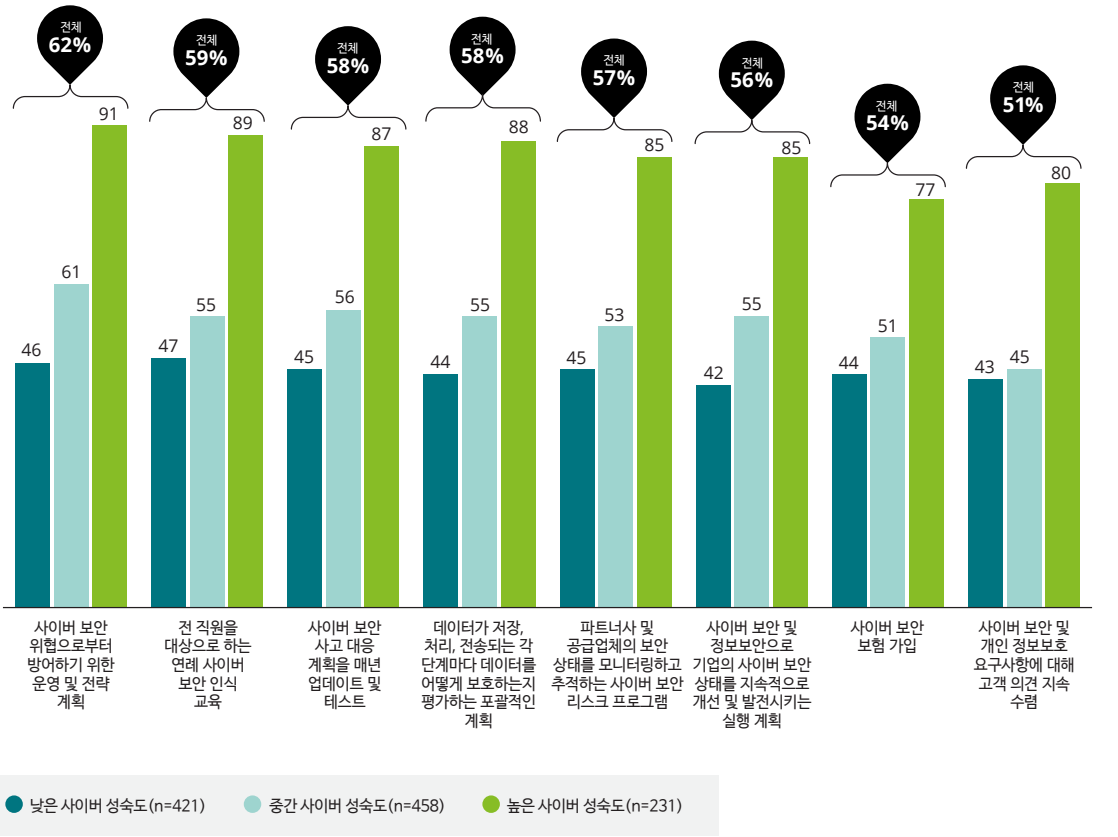
91%의

사이버 성숙도가 높은 기업은 사이버 위협으로부터 방어하기 위한 운영 및 전략적 계획 수립하고 있음

그림 9. 다양한 사이버 성숙도 그룹의 계획 현황

해당 조치를 완전히 실행하고 있는 기업

(단위: %)



4. 인재에 대한 이해 및 투자

사이버 이슈와 활동은 결국 '사람'으로 귀결된다. 취약점을 악용하려는 공격자든, 사이버 전략과 전술을 책임지는 의사 결정자든, 디지털 비즈니스 프로세스와 사이버 프로그램을 운영하는 실무자든 결국 모두 사람이 하는 일이다. 강력한 인력, 즉 경험이 풍부하고 노련하며 사이버에 집중하는 인력은 좋은 성과를 내는 데 필수 조건이다. 사이버 이니셔티브를 추진할 수 있는 적절한 인력을 확보하기 위해서는 직원들의 기존 프로필에 국한하여 생각하기보다 고정관념을 깨고 틀에 박힌 사고방식에서 벗어나야 한다. 예를 들어 고객 경험 설계자는 사이버 이니셔티브에 필요한 통찰력을 제공하여 트랜잭션 프로세스, 데이터 수집, 개인 정보 보호와 관련된 잠재적 취약성을 파악하는 데 도움이 될 수 있다.

적절한 인재를 유치하고 유지하기란 어려운 일이다. 사이버에 관한 어떤 직책이든 자연스레 강한 강도의 스트레스와 압박감이 따라온다. 본 연구의 일환으로 한 영국 금융 업계의 리더를 인터뷰한 결과, 그는 자신의 '고위 관리자'라는 직함이 뜻하는 바는 사실상 CISO와 함께 사이버 리스크에 대한 책임이 있으며, 경우에 따라서는 "개인에게 심각한 결과를 초래할 수 있다"는 것이라고 지적했다. 이는 기업들이 사이버에 집중하고 있음을 나타내며, 또한 사이버에 대한 책임이 단 하나의 직함이나 부서에 국한되지 않아야 함을 뜻한다.

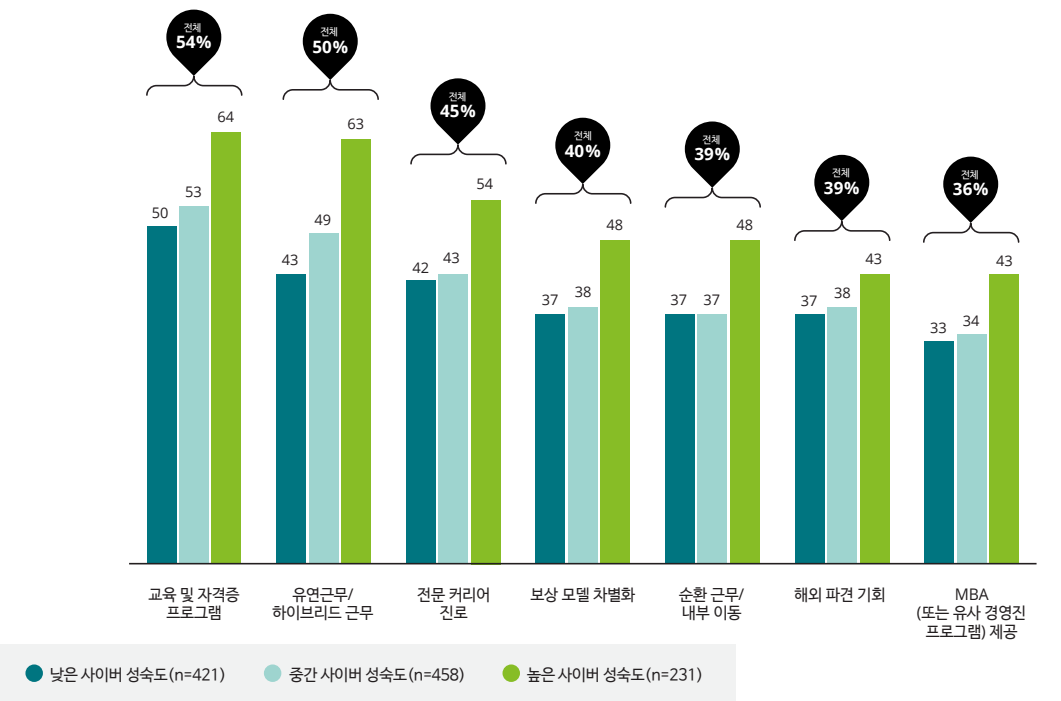
전반적으로 성숙도가 높은 기업은 사이버 활동에 있어 숙련된 인재의 중요성을 높이 평가하고 있으며 가치 있는 인재를 유지하기 위해 유의미한 조치를 취하고 있다. 성숙도가 높은 기업은 사이버 관리의 최우선 문제로 숙련된 사이버 전문가 부족을 꼽는 경향이 훨씬 크다(성숙도 높은 기업 47%, 중간 기업 38%, 낮은 기업 37%).

성숙한 기업의 경우 고도화된 사이버 프로그램이 인력 부족 문제의 일부가 될 수 있다. 사이버 관련 활동을 보다 폭넓고 심층적으로 진행하면서 팀과 역량을 최대치로 사용하기 때문에 보다 성숙한 프로그램을 지원하기 위한 다양한 고급 기량을 가진 인재를 유치할 필요성을 느낄 수 있다.

하지만 성숙도가 낮은 기업들은 동일한 인력 문제를 겪고 있지 않는 것일까? 아니면 단순히 적절한 기량을 갖추는 데 중점을 두지 않는 것일까? 후자의 경우라면 인재 확보를 강조하는 것이 우선시되어야 한다. 인재 확보는 보다 성숙한 기업으로 나아가는 데 도움이 될 수 있기 때문이다(그림 10).

그림 10. 기존 인재의 참여, 유지, 개발을 위해 기업이 취하는 전략

(단위: %)



5. 도구와 서비스의 다양한 생태계

성숙도가 높은 기업들은 사이버의 미래를 주도하고자 하는데 이들은 이를 자체적으로 할 수 없다는 점을 정확히 알고 있다. 이들은 비즈니스 가치를 지탱할 수 있는 미래 지향적인 사이버 역량을 갖추기 위해 기술과 역량, 외부 오퍼링으로 이뤄진 폭넓은 외부 생태계의 힘을 빌려야 한다.

성숙도가 낮거나 중간 수준인 기업들에 비해 성숙도가 높은 기업은 다음과 같은 타사 제품 및 서비스를 활용하는 경향이 크다 (그림 11).

- 애플리케이션 보안
- 사이버 클라우드
- 사이버 전략
- 데이터 및 개인 정보 보호
- 탐지 및 대응
- 신기술(OT, 5G, AI, 양자 컴퓨팅)
- ID 및 접근 권한 관리
- 인프라 보안
- 복구 및 전환

이러한 도구와 서비스를 활용하면 사이버 역량을 키울 수 있으나 탄탄한 생태계 계획, 관리, 운영에 대한 필요성이 생긴다. 여러 업체와 협력하여 진화하는 복잡한 문제를 해결하고 사이버 역량을 실행, 모니터링, 업데이트하다 보면 새롭고 복잡한 니즈가 생겨난다.

아이러니하게도 여러 사이버 업체와 협업하면서 발생하는 복잡성으로 인해 새로운 리스크가 발생할 수 있는 것이다. 상황에 따라 외부업체 감독 업무를 통합하여 문제를 단순하게 만드는 것도 방법이다.

향후 2년 내에 기업마다 평균적으로 활용하는 외부업체의 수가 증가할 것으로 예상됨에 따라 관리 감독을 단순화하고 통합하는 사례 또한 증가할 것으로 보인다. 고려해볼 만한 또 다른 접근법은 산업 단체 등의 기관과 협력하는 것이다. 생태계를 관리하는 방법에 영향을 미칠 수 있는 기술 발전과 새로운 관행에 대해 더 잘 이해할 수 있다.

행동의 변화

직원들의 잠재적인 사이버 리스크 지표를 감지하여 완화할 수 있는 자동 행동 분석 도구의 사용이 크게 증가했다. 2021년 조사에서는 응답자 중 53%가 이러한 도구를 사용했다고 답했는데, 금번 조사에서 무려 76%가 사용했다고 응답했다.

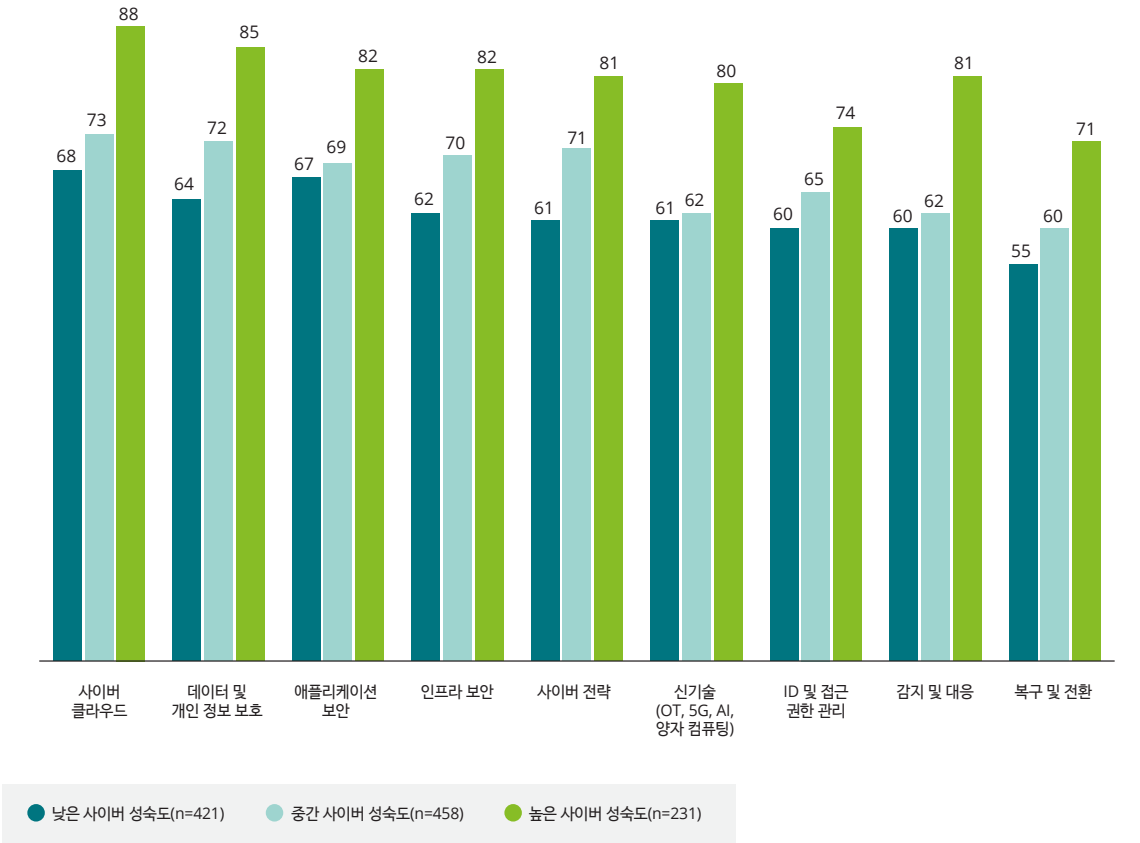
새로운 관점 확보

"100% 내부화 전략은 통하지 않습니다. 확장성도 없고요. 현실과 동떨어지게 되는 경향이 있죠. 저희는 다양한 파트너사와 협업하고 있습니다. 새로운 아이디어를 얻고 전략적으로 방향을 잡는 데 도움이 됩니다."

자동차 기업 CISO

그림 11. 기업들이 외부 사이버 서비스 업체를 활용하는 영역

(단위: %)



전망

기업 리더들이 회사가 커지고 성장하기를 기대한다면 사이버가 계획의 필수 요소가 되리라는 것을 예상해야 한다. 사이버는 또한 앞으로 사업 목표를 위해 사용할 모든 도구의 필수적인 요소가 되어야 한다.

사이버를 뒷전으로 미루는 시대는 지났다. 그리고 어떤 사업이든 탄탄한 사이버 전략을 마련할 때 새로운 기술 역량의 효과가 커질 것이다. 신기술은 미래 사업 모델에 도움이 되며 사이버 일선에서 예상치 못한 문제를 제시할 수 있는 혁신적인 솔루션을 가져올 것이다. 비즈니스 가치를 위해 이러한 기술을 활용하는 동시에 사이버 전략과 투자가 발을 맞추려면 어떻게 해야 할까?

우선 제로 트러스트 접근법이 중심이 되어야 한다. 제로 트러스트는 보안 아키텍처에서 '신뢰'를 기본 가정으로 삼았던 기존의 접근법을 버리고 모든 작업과 사용자, 장치에 대해 인증 과정을 거친다. 그렇게함으로써 보다 강력하고 회복탄력적인 보안 상태를 가능하게 한다. 엔드 유저는 업무를 효율적으로 하는 데 필요한 도구와 데이터에 원활하게 접근할 수 있다.

"제로 트러스트로 전환하는 과정은 대규모 IT 자산을 가진 저희와 같은 회사의 경우 매우 복잡해집니다. 다양한 워크로드를 처리하기 위해 많은 종류의 기기와 연결하고자 하는 파트너사 생태계는 계속해서 커져가고 있는데, 이에 따른 복잡성을 관리하면서 동시에 비즈니스의 속도에 맞게 혁신해야 합니다. 그리고 이 모든 것을 안전하게 진행해야 하죠."

쉘(Shell)사 CIO/CISO 앨런 콕리얼

"저희는 보다 다양한 디지털 솔루션을 보유하게 될 것입니다. 여기에는 AI와 슈퍼 컴퓨팅과 같이 어떤 사업에 특수하거나 데이터 집약적인 솔루션이 포함됩니다. 그렇게 되려면 저희 사이버 환경이 효과적으로 보호받고 있는지, 규제 기준을 충족하고 있는지 등에 대한 지속적인 업데이트가 필요하죠."

BASF 데이터 보호 책임자, 찰리 황

혁신을 시작할 때는 전략 수립부터 시작하여 사이버 관점에서 그 전략에 도움이 될 수 있는 기술에 대해 이해한 후 비판적인 시각으로 이를 평가해야 한다. 예를 들어, 데이터 서비스나 플랫폼을 사용하는 것이 어떻게 목적에 부합하고 신뢰를 쌓는 능력을 늘리는지, 그리고 어떻게 기업을 리스크와 위협에 노출시킬 수 있는지의 측면에서 평가해야 한다. 그 후 적절한 요구사항에 대한 적절한 솔루션을 적용해야 할 것이다.

내다보며

새로운 기술에 내재된 리스크와 기회를 감지하는 것은 진화하는 위협을 따라잡을 수 있는 한 방법이다. 기업들은 빠르게 바뀌는 기술 트렌드를 따라잡기에만 급급하기를 원하지 않을 것이다. 기술 변화에 대한 준비가 부족할수록 사이버 리스크 관리에 대한 준비가 부족해진다.

대표적인 사례가 그 중요성이 높아지고 있는 5G이다. 5G는 금번 서베이에서 디지털 전환 이니셔티브 상위 5위권에 새로 진입했다. 5G는 원격 의료, 제조업에서의 자산 추적(asset tracking), 고급 교육을 위한 증강 현실과 같은 새로운 사용 사례를 가능하게 할 수 있지만, 5G로 인해 공격 노출면이 커지기도 한다[7]. 처음부터 보안을 설계하고 적용하는 것은 5G 채택에 매우 중요하지만[8] 매우 복잡할 것이다.

한편 서베이 결과 확인된 Top 5 디지털 전환 이니셔티브 중 인공지능(AI)은 기업이 사이버를 포함해 다양한 분야에서 복잡성을 해결하는 데 도움이 될 수 있다. 기업들이 보안 사고로 어려움을 겪을 때 사이버 AI(Cyber AI)는 강력한 힘을 발휘할 수 있으며 이를 통해 보안 팀은 사이버 공격에 더 빠르게 대응할 수 있을 뿐만 아니라 이러한 움직임을 예측하고 사전에 조치를 취할 수 있다[9]. 기업들은 AI와 자동화를 통해 분석가들의 따분한 업무를 줄일 수 있으며, 보다 전략적인 역할을 맡도록 교육할 수 있다[10].

그리고 서베이 응답자 중 4%만이 향후 몇 년 안에 디지털 이니셔티브 중 우선 순위가 될 것이라고 응답한 양자 컴퓨팅을 포함해, 훨씬 더 먼 미래의 기술에 대해 가능한 빨리 고려하기 시작해야 한다. 기업은 양자 컴퓨팅으로 엄청난 연산 능력을 확보할 수 있지만 사이버 공격자가 활용할 수 있는 도구 또한 제공할 수 있다. 따라서 양자 컴퓨팅에 대비하는 새로운 기반이 필요하다[11].

설계별 보안

"실제로 저희는 이른바 '보안 내재화'(secure by design)에 투자해서 저희 가치 제안의 수많은 요소에 보안이 포함될 수 있도록 하고 있습니다. 저희는 훌륭하고 안전한 기술을 만들기 위해 소프트웨어 및 제품 라이프 사이클 전반적으로 정책, 툴링(tooling), 제어 등에 투자하고 있습니다. 고객들이 이를 기대하기 때문입니다."

쉘(Shell)사 CIO/CISO 앨런 콕리얼

나아가며

사이버의 미래와 사업의 미래는 서로 밀접하게 얽혀 있다. 사이버 사고, 계획, 행동을 어떻게 비즈니스 이니셔티브에 포함시키는지에 따라 성공 여부가 결정된다.

사이버는 토대이다. 사이버는 디지털 신뢰를 실현하고 유지하기 위한 기반으로, 비즈니스의 미래가 이 위에 세워질 것이다. 비즈니스가 디지털 영역으로 점점 더 급격하게 이동함에 따라, 효과적인 디지털 생태계의 구축은 비즈니스 성과를 이끄는 효과적인 사이버 전략을 수립하는 데 달려 있다.

브랜드 평판. 고객의 신뢰와 충성도. 운영 안정성. 매출 증가. 이 모든 것은 사이버를 얼마나 잘 계획하고 실행하느냐에 달려 있다. 즉, 사이버 기반을 얼마나 탄탄하게 다지느냐에 달려 있는 것이다. 새로운 클라우드 이니셔티브를 시작할 때, 자사의 생태계에 외부 업체를 추가할 때, 또는 직원에게 새로운 도구를 제공할 때 등 여러 경우에 사이버를 우선시하는 것이 필수적이다. 사이버는 통찰력, 플랫폼, 연결성, 무결성 등 여러 디지털 필수 요소보다 중요하다.

시작하기

사이버에 대한 당신의 접근법에는 사업의 미래에 어떻게 접근할 것인지, 그리고 사업 목표를 얼마나 잘 달성할 것인지 등 많은 것이 담겨있다. 현재 귀사가 어디에 있든, 어디로 나아가기를 원하든, 무엇이 가능하고 무엇이 앞길에 놓여있을지에 대해 명확히 이해하고 시작하는 것이 도움이 될 것이다.

감사의 말

Ian Blatchford, Scott Buzik, Luca Covolo, Deborah Elder, Jaya Gopalan, Jeremy Guterl, Matthew Holt, Dan Konigsburg, Daphne Lucas, Diana Kearns-Manolatos, Emily Mossburg, Mike Nash, Kelly Nelson, Jud Payne, Sean Peasley, Ashley Reichheld, Heather Saxon, Daniel Soo, Scott Tillett, Niels van de Vorle, Marius von Spreti, Emily Werner

Contacts

서영수

딜로이트 안진회계법인 사이버 리더

youngseo@deloitte.com
+82 2 6676 1929

유선희

딜로이트 안진회계법인 사이버 파트너

sunhyou@deloitte.com
+82 2 6676 2956

주석

1. Deloitte 2021 Future of Cyber Survey.
2. Closing the cloud strategy, technology, and innovation gap. Deloitte US Future of Cloud Survey Report, 2022.
3. Future of Digital Trust: Driving forces, trends and their implications on our digital tomorrow. Deloitte. 2021.
4. The Four Factors of Trust: How Organization Can Earn Lifelong Loyalty.
5. Ibid
6. Fueling the AI transformation: Four key actions powering widespread value from AI, right now. Deloitte's State of AI in the Enterprise, 5th Edition report, October 2022.
7. Take 5: 5G cybersecurity, Part of Deloitte's 'Take 5 on 5G' article series.
8. Ibid
9. Cyber AI: Real Defense, Deloitte Tech Trends 2022.
10. Ibid
11. Quantum Cyber Readiness Deloitte's perspective on transitioning to a quantum secure economy

원문 바로보기

Deloitte.
Insights

딜로이트 안진회계법인·딜로이트 컨설팅
고객산업본부

손재호 Partner
고객산업본부 본부장
jaehoson@deloitte.com

정동섭 Partner
딜로이트 인사이트 리더
dongjeong@deloitte.com

김사현 Director
딜로이트 인사이트 편집장
sahekim@deloitte.com

HOT LINE
02) 6099-4651